(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 198 04 054 B4** 2010.04.01

(12) **Patentschrift**

(21) Aktenzeichen: **198 04 054.7**
(22) Anmeldetag: **03.02.1998**
(43) Offenlegungstag: **27.08.1998**
(45) Veröffentlichungstag der Patenterteilung: **01.04.2010**

(51) Int Cl.[8]: ***H04L 9/32*** (2006.01)

Innerhalb von drei Monaten nach Veröffentlichung der Patenterteilung kann nach § 59 Patentgesetz gegen das Patent Einspruch erhoben werden. Der Einspruch ist schriftlich zu erklären und zu begründen. Innerhalb der Einspruchsfrist ist eine Einspruchsgebühr in Höhe von 200 Euro zu entrichten(§ 6 Patentkostengesetz in Verbindung mit der Anlage zu § 2 Abs. 1 Patentkostengesetz).

(30) Unionspriorität:
9702152 03.02.1997 GB

(73) Patentinhaber:
Certicom Corp., Mississauga, Ontario, CA

(74) Vertreter:
Flaccus, R., Dipl.-Chem. Dr.rer.nat., Pat.-Anw., 50389 Wesseling

(72) Erfinder:
Vanstone, Scott A., Waterloo, Ontario, CA

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

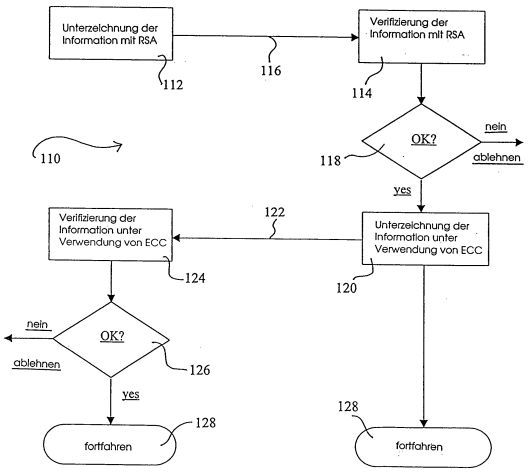
US	**53 96 558**	**A**
EP	**04 40 800**	**A1**
US	**49 95 082**	**A**

(54) Bezeichnung: **System zur Verifizierung von Datenkarten**

(57) Hauptanspruch: Verfahren zur Verifizierung der Echtheit von zwischen einem Teilnehmerpaar in elektronischen Transaktionen über ein Datenübertragungssystem ausgetauschten Nachrichten, wo bei jeder der Teilnehmer Unterzeichnungs- und Verifizierungsteile eines ersten Unterschriftsschemas und eines zweiten Unterschriftsschemas, das sich vom ersten Unterschriftsschema unterscheidet und ein Verschlüsselungssystem mit elliptischer Kurve verwendet, aufweist, und wobei das Verfahren die folgenden Schritte umfasst:

die Unterzeichnung einer Nachricht durch einen der Teilnehmer gemäss einem Unterzeichnungsteil eines der Unterschriftsschemas, das mit dem Teilnehmer verbunden ist, um eine erste unterzeichnete Nachricht bereitzustellen, und Übertragung der ersten unterzeichneten Nachricht an den anderen der Teilnehmer; wobei der genannte andere Teilnehmer den Verifizierungsteil des genannten einen Unterschriftsschemas verwendet, um die von dem genannten einen Teilnehmer empfangene erste un terzeichnete Nachricht zu verifizieren;

die Unterzeichnung einer Nachricht durch den genannten anderen Teilnehmer unter Verwendung des genannten Unterzeichnungsteils des genannten anderen der Unterschriftsschemas, um eine zweite unterzeichnete Nach richt bereitzustellen, und Übertragung der zweiten unterzeichneten...



Beschreibung

[0001] Die Erfindung betrifft Verfahren und Vorrichtungen für den Datentransfer und die Authentisierung von Daten in einem System für elektronische Transaktionen, und insbesondere elektronische Transaktionssysteme mit Verwendung von Chipkarten.

[0002] Die Durchführungen von Transaktionen wie finanzielle Transaktionen oder Dokumentenaustausch auf elektronischem Wege hat weite Akzeptanz gefunden. Automatische Schaltermaschinen (ATMs, "automated teller machines") und Kreditkarten werden häufig für persönliche Transaktionen verwendet, und mit steigender Häufigkeit der Verwendung steigt auch der Bedarf an einer Überprüfung solcher Transaktionen. Eine Chipkarte hat in etwa Ähnlichkeit mit einer Kreditkarte und enthält eine gewisse Rechen- und Speicherkapazität. Chipkarten unterliegen der Gefahr des betrügerischen Mißbrauchs, z. B. durch Terminalattrappen, die dazu verwendet werden, Informationen von einem arglosen Anwender auszuspähen. Daher ist vor einem Austausch wichtiger Informationen vom Terminal zur Chipkarte oder vice versa die Verifizierung der Echtheit des Terminals wie auch der Chipkarte notwendig. Eine dieser Verifizierungen kann in Form von einer digitalen "Unterzeichnung" einer anfänglichen Transaktion stattfinden, so daß die Echtheit der Transaktion von beiden an der nachfolgenden Sitzung beteiligten Parteien geprüft werden kann. Die Unterschrift wird gemäß einem Protokoll ausgeführt, welches eine Zufallsnachricht verwendet, das heißt die Transaktion und einen Geheimschlüssel, der mit der Partei assoziiert ist.

[0003] Die Unterschrift muß so durchgeführt werden, daß der geheime Schlüssel der Partei nicht ermittelt werden kann. Um die Komplexität der Verteilung von Geheimschlüsseln zu vermeiden, ist die Verwendung von Verschlüsselungsverfahren mit öffentlichen Schlüsseln für die Generierung der Signatur zweckmäßig. Solche Kapazitäten sind dort vorhanden, wo die Transaktionen zwischen Parteien stattfinden, die Zugang zu relativ großen Rechnerkapazitäten haben, jedoch ist es von ebenso großer Bedeutung, derartige Transaktionen auch auf einer individuellen Ebene – wo begrenztere Rechenkapazitäten zur Verfügung stehen, wie im Falle der Chipkarte – zu erleichtern.

[0004] US 5 396 558 A beschreibt ein Protokoll zwischen einer Chipkarte und einem Terminal zur gegenseitigen Authentifizierung. Auf der Chipkarte sind ein öffentlicher Hauptschlüssel nA zum Überprüfen einer digitalen Hauptsignatur SA, eine Kartenidentifikationsnummer IDU sowie eine erste digitale Hauptsignatur SA1 gespeichert. Im Kartenterminal sind der bereits erwähnte Hauptschlüssel nA, eine Terminal-Identifikationsnummer IDT, sowie eine zweite digitale Hauptsignatur SA2 gespeichert.

[0005] Das Authentifizierungsverfahren umfaßt: einen Schritt, bei dem die Chipkarte die IDU und die erste digitale Hauptsignatur SA1 an das Terminal übermittelt; einen Schritt, bei dem das Kartenterminal die Gültigkeit der Signatur SA1 durch Anwendung des öffentlichen Hauptschlüssels nA und der von der Karte empfangenenen IDU überprüft; einen Schritt, bei dem das Terminal IDT und SA2 an die Karte übermittelt, wenn SA1 gültig ist; einen Schritt, bei dem die Karte die Gültigkeit der zweiten digitalen Hauptsignatur SA2 durch Anwendung des öffentlichen Hauptschlüssels nA und der vom Kartenterminal empfangenen IDT überprüft.

[0006] Bei dem Authentifizierungsprotokoll wird jeweils nur ein Signaturschema verwendet, z. B. DSA.

[0007] EP 0 440 800 A1 beschreibt ein Protokoll zur gegenseitigen Authentifizierung zwischen einer Benutzerkarte und einer SA(Security Authentication)-Karte. Bei dem Verfahren wird ein gemeinsamer geheimer Schlüssel K1 für die Authentifizierung der Benutzerkarte durch die SA-Karte, und ein gemeinsamer geheimer Schlüssel K2 für die Authentifizierung der SA-Karte durch die Benutzerkarte verwendet. Die SA-Karte erzeugt Zufallszahlen R1 und sendet diese an die Benutzerkarte. Letztere generiert verschiedene Zufallszahlen R2, die von der SA-Karte mittels des Schlüssels K2 verschlüsselt werden, und das Ergebnis F(K2, R2) wird an die Benutzerkarte gesendet. Die Benutzerkarte vergleicht dann dieses Ergebnis mit dem Ergebnis, das sie selbst durch Verschlüsselung für R2 erhalten hat. Wenn die Authentifizierung korrekt ist, verschlüsselt die Benutzerkarte R1 mit K1 und sendet das Ergebnis F(K1, R1) an die SA-Karte, die ebenfalls R1 mit K1 verschlüsselt und durch Vergleich des Ergebnisses die Benutzerkarte authentifiziert.

[0008] US 4 995 082 beschreibt ebenfalls ein Verfahren zur gegenseitigen Authentifizierung zwischen einem Terminal und einer Karte. Zur Vereinfachung der Berechnungen auf der Karte wird vorgeschlagen, daß die Länge der benutzten Schlüssel entsprechend kurz sein soll. Es werden zwar zwei unterschiedliche Signaturverfahren erwähnt, jedoch entspricht keines dieser Verfahren einem Elliptic-Curve-Kryptosystem (ECC).

[0009] Transaktionskarten oder Chipkarten sind derzeit mit begrenzter Rechenkapazität erhältlich, diese sind jedoch für eine wirtschaftliche Umsetzung existierender digitaler Unterschriftsprotokolle nicht ausreichend. Wie oben bemerkt, erfordert die Erzeugung einer Verifizierungsunterschrift die Verwendung eines Verschlüsselungsverfahrens mit öffentlichem Schlüssel. Derzeit basieren die meisten Verfahren mit öffentlichem Schlüssel auf RSA, doch findet hier

durch DSS und den Bedarf an einem kompakteren System eine rapide Veränderung statt. Das DSS-Verfahren, das eine Umsetzung eines Diffie-Hellman-Protokolls mit öffentlichem Schlüssel darstellt, versendet eine Menge von ganzen Zahlen Z_p, wobei p eine große Primzahl ist. Um eine adäquate Sicherheit zu erzielen, muß p in der Größenordnung von 512 bit liegen, allerdings kann die resultierende Signatur mod q reduziert werden, wobei sich q aufgliedert in p – 1, und in der Größenordnung von 160 bit liegen kann.

[0010] Ein alternatives Verschlüsselungsverfahren, das eins der ersten voll ausgereiften Algorithmen mit öffentlichem Schlüssel darstellte, und daß sowohl für Verschlüsselungen wie auch für die digitale Unterzeichnung geeignet ist, ist als RSA-Algorithmus bekannt. Bei RSA basiert die Sicherheit auf der Schwierigkeit, große Zahlen zu faktorisieren. Die öffentlichen und privaten Schlüssel sind Funktionen von Paaren von großen (100- bis 200stellig oder noch größer) Primzahlen. Der öffentliche Schlüssel für RSA-Verschlüsselung ist n, nämlich das Produkt der zwei Primzahlen p und q, wobei p und q geheim bleiben müssen, und e, das zu $(p – 1) \times (q – 1)$ relativ teilerfremd ist. Der Verschlüsselungsschlüssel d ist gleich $e^{-1} \pmod{(p – 1) \times (q – 1)}$. Man bemerke, daß d und n relativ teilerfremd sind.

[0011] Um eine Nachricht m zu verschlüsseln, wird diese zuerst so in eine Anzahl von numerischen Blöcken unterteilt, daß jeder Block eine einzigartige Darstellung nach Modulo n ist, dann ist der verschlüsselte Nachrichtenblock c_i einfach $m_i^c \pmod{n}$. Zur Entschlüsselung einer Nachricht wird jeder verschlüsselte Block c_i genommen und $m_i = c_i^d \pmod{n}$ errechnet.

[0012] Ein anderes Verschlüsselungsverfahren, das erhöhte Sicherheit bei relativ kleinem Modul bereitstellt, verwendet elliptische Kurven im endlichen Feld 2^m. Ein Wert von m in der Größenordnung von 155 bietet eine Sicherheit, die mit einem 512 bit Modul DSS vergleichbar ist, und bietet daher bedeutende Vorteile für die Umsetzung.

[0013] Diffie-Hellman-Verschlüsselung mit öffentlichem Schlüssel verwendet die Eigenschaften von diskreten Logarithmen, so daß selbst bei bekanntem Generator ß und bekannter Potenzierung $ß^k$ der Wert von k nicht bestimmt werden kann. Eine ähnliche Eigenschaft weisen elliptische Kurven auf, bei denen die Addition von zwei Punkten auf einer Kurve einen dritten Punkt auf dieser Kurve ergibt. In ähnlicher Weise wird durch Multiplikation eines Punktes P auf der Kurve mit einer ganzen Zahl k ein weiterer Punkt auf der Kurve erzeugt. Für eine elliptische Kurve wird der Punkt kP einfach durch Zusammenaddieren von k Kopien des Punktes P erhalten.

[0014] Jedoch enthüllt die Kenntnis des Startpunktes und des Endpunktes nicht den Wert der ganzen Zahl k, die dann als Sitzungsschlüssel für die Verschlüsselung verwendet werden kann. Der Wert kP, wobei P ein bekannter Anfangspunkt ist, ist daher äquivalent zu der Potenzierung $ß^k$.

[0015] Darüber hinaus bieten Verschlüsselungssysteme mit elliptischen Kurven Vorteile gegenüber anderen Verschlüsselungssystemen, wenn Bandbreiteneffizienz, reduzierter Rechenaufwand und minimierter Coderaum zu den Anwendungszielen gehören.

[0016] Weiterhin sind im Kontext der Chipkarten- und Schalterautomaten-Transaktionen zur Authentisierung der beiden Parteien zwei Hauptschritte nötig. Der erste ist die Authentisierung des Terminals durch die Chipkarte und der zweite die Authentisierung der Chipkarte durch das Terminal. Generell erfordert die Authentisierung die Überprüfung eines Zertifikates, das vom Terminal erzeugt und von der Chipkarte empfangen wird, sowie die Überprüfung eines Zertifikates, das von der Chipkarte unterzeichnet wurde und vom Terminal geprüft wird. Sobald die Zertifikate positiv verifiziert sind, kann die Transaktion zwischen der Chipkarte und dem Terminal fortgeführt werden.

[0017] Aufgrund der begrenzten Rechenkapazität der Chipkarte, sind die Prüfungen und die Verarbeitung der Unterschrift, die auf der Chipkarte durchgeführt werden, im allgemeinen auf einfache Verschlüsselungsalgorithmen begrenzt. Ein höher entwickelter Verschlüsselungsalgorithmus übersteigt im allgemeinen die Möglichkeiten der in der Karte enthaltenen Rechenkapazitäten. Es besteht daher ein Bedarf an einem Verfahren zur Unterschriftsprüfung und -erzeugung, das auf einer Chipkarte implementiert werden kann, und das relativ sicher ist.

[0018] Die Erfindung zielt in einer Hinsicht auf die Bereitstellung eines Verfahrens zur Datenverifizierung zwischen einer Chipkarte und einem Terminal.

[0019] In Übereinstimmung mit diesem Aspekt wird ein Verfahren zur Verifizierung eines Paares von Teilnehmern an einer elektronischen Transaktion bereitgestellt, das folgende Schritte umfaßt:
Überprüfung von Information, die der zweite Teilnehmer vom ersten Teilnehmer empfangen hat, wobei die Prüfung gemäß einem ersten Unterschriftsalgorithmus erfolgt;
Überprüfung von Information, die der erste Teilnehmer vom zweiten Teilnehmer empfangen hat, wobei die Prüfung gemäß einem zweiten Unterschriftsalgorithmus; und
wobei die Transaktion verweigert wird, falls eine der Prüfungen negativ ausfällt.

[0020] Der erste Signaturalgorithmus kann ein solcher sein, bei dem die Unterzeichnung rechnerisch

schwieriger ist als die Verifizierung, während bei dem zweiten Unterschriftsalgorithmus die Verifizierung schwieriger ist als die Unterzeichnung. Bei einer solchen Ausführungsform kann der zweite Teilnehmer mit relativ geringer Rechenkapazität teilnehmen, während die Sicherheit auf hohem Niveau bestehen bleibt.

[0021] In einer weiteren Ausführungsform basiert der erste Signaturalgorithmus auf einem RSA- oder DDS-Algorithmus und der zweite Signathuralgorithmus auf einem Algorithmus mit elliptischer Kurve.

[0022] Eine Ausführungsform der Erfindung wird im folgenden beispielhaft mit Bezug auf die beigefügten Zeichnungen beschrieben. Die Zeichnungen zeigen:

[0023] Fig. 1a: eine schematische Darstellung einer Chipkarte und eines Terminals;

[0024] Fig. 1b: eine schematische Darstellung der Abfolge von Ereignissen, die während des Verifizierungsvorganges in einem Chipkarten-Transaktionssystem ablaufen; und

[0025] Fig. 2: eine detaillierte schematische Darstellung eines spezifischen Protokolls.

[0026] Unter Bezugnahme auf **Fig.** 1(a), ist ein Terminal **100** für die Aufnahme einer Chipkarte **102** ausgebildet. Typischerweise startet das Einführen der Karte **102** in das Terminal die Transaktion. Die gegenseitige Authentisierung zwischen Terminal und Karte erfolgt dann wie in Fig. 1b gezeigt. Sehr allgemein gesprochen erfolgt diese gegenseitige Authentisierung gemäß einem ”Abfrage-Antwort”-Protokoll. Generell übermittelt die Karte eine Information an das Terminal, das Terminal **100** unterzeichnet die Information mit einem Algorithmus **112** auf RSA-Basis und sendet sie dann an die Karte **102**, die die Information mit einem auf RSA basierenden Algorithmus **114** überprüft. Der Informationsaustausch **116** zwischen der Karte und dem Terminal beinhaltet ebenfalls die von der Karte erzeugte Information, die an das Terminal zur Unterzeichnung durch dieses mit einem RSA-Algorithmus geschickt wird, und die zur Karte zurückgeschickt wird zur Verifizierung mittels eines RSA-Algorithmus. Sobald die betreffende Verifizierung abgeschlossen ist **118**, wird ein weiterer Schritt durchgeführt, in dem die Information von der Karte unter Verwendung eines Verschlüsselungsprotokolls **120** mit elliptischer Kurve unterzeichnet wird und an das Terminal zur Verifizierung **124** durch das Terminal unter Verwendung eines auf einer elliptischen Kurve basierenden Protokolls weitergeleitet wird.

[0027] In ähnlicher Weise kann der Informationsaustausch **122** zwischen der Karte und dem Terminal vom Terminal generierte Information beinhalten, die an die Karte zur Unterzeichnung durch dieselbe geschickt und zum Terminal zur Verifizierung zurückgeschickt wird. Sobald die betreffende Information überprüft **126** wurde, können die weiteren Transaktionen zwischen Terminal und Karte fortgeführt **128** werden.

[0028] Unter Bezugnahme auf Fig. 2, wird eine detaillierte Umsetzung der gegenseitigen Authentisierung des Terminals und der Karte gemäß dem ”Abfrage-Antwort”-Protokoll generell mit dem Bezugszeichen **200** bezeichnet. Das Terminal **100** wird zuerst durch die Karte **102** verifiziert, und die Karte wird dann durch das Terminal verifiziert. Das Terminal sendet zunächst ein Zertifikat C_1, **20**, das dessen ID, T_{ID}, sowie öffentliche Informationen einschließlich eines öffentlichen Schlüssels enthält, an die Karte. Das Zertifikat **20** kann auch von einer ein Zertifikat ausstellenden Berechtigungsstelle (CA, ”certifying authority”) unterzeichnet werden, so daß die Karte, die Assoziierung des Terminals ID T_{ID} mit dem vom Terminal erhaltenen öffentlichen Schlüssel überprüfen kann. Die vom Terminal und der CA verwendeten Schlüssel können bei dieser Ausführungsform beide auf einem RSA-Algorithmus basieren.

[0029] Beim RSA-Algorithmus hat jeder Teilnehmer bzw. jede Partei einen öffentlichen und einen privaten Schlüssel, und jeder Schlüssel hat zwei Teile. Die Unterschrift hat die Form:

$$S = m^d \pmod n,$$

wobei gilt:

- m ist die zu unterzeichnende Nachricht;
- n, der öffentliche Schlüssel, ist der Modul und das Produkt von zwei Primzahlen p und q;
- e ist der Verschlüsselungschlüssel, der zufällig gewählt und ebenfalls öffentlich ist; er ist eine gewählte Zahl, die zu $(p-1) \times (q-1)$ relativ teilerfremd ist; und
- d ist der private Schlüssel, der mit $e^{-1} \pmod{(p-1) \times (p-1)}$ kongruent ist.

[0030] Für den RSA-Algorithmus ist das Paar ganzer Zahlen (n, e) die Information des öffentlichen Schlüssels, die zur Unterzeichnung verwendet wird, während das Paar ganzer Zahlen (d, n) zur Entschlüsselung einer Nachricht verwendet werden kann, die mit der Information des öffentlichen Schlüssels (n, e) verschlüsselt wurde.

[0031] Unter Bezug auf Fig. 2, stellen die Zahlen n und e die öffentlichen Schlüssel der CA dar und können als Systemparameter gesetzt werden. Der öffentliche Schlüssel e kann entweder in der Chipkarte oder in einer alternativen Ausführungsform in einen Logikschaltkreis in der Karte eingebunden sein. Darüber hinaus ermöglicht die Wahl eines relativ kleinen e eine relativ schnelle Durchführung der Potenzie-

rung.

[0032] Das Zertifikat **20** C_1 wird von der CA unterschrieben und hat die Parameter (n, e). Das Zertifikat enthält die Terminal-ID, T_{ID}, und die Information des öffentlichen Schlüssels des Terminals T_n and T_e, die auf dem RSA-Algorithmus basiert. Das Zertifikat C_1 wird von der Karte durch Extrahieren von T_{ID}, T_n, T_e geprüft **24**. Diese Information wird einfach durch Ausführen von C_1^emod n extrahiert. Die Karte authentisiert dann das Terminal durch Generieren einer Zufallszahl R1, **26**, die sie zum Terminal überträgt. Das Terminal unterzeichnet die Nachricht R1 unter Verwendung seines geheimen Schlüssels T_d durch Ausführen von $R1^{Td}$ $MODT_n$ zur Erzeugung des Wertes C_2, **28**. Der von dem Terminal verwendete Schlüssel ist wieder ein RSA-Schlüssel, der ursprünglich so generiert wurde, daß der öffentliche Schlüssel T_e aus einem kleinen, möglicherweise systemweiten Parameter mit dem Wert 3 besteht, während der andere Teil des öffentlichen Schlüssels der Modul T_n ist, der mit dem Terminal assoziiert wird. Der private Schlüssel T_d kann nicht klein sein, wenn er einem kleinen öffentlichen Schlüssel T_e entspricht. Im Falle des Terminals ist es nicht von Bedeutung, ob ein großer privater Schlüssel T_d gewählt wird, da das Terminal über die erforderliche Rechenkapazität für eine relativ schnelle Durchführung der Potenzierung verfügt.

[0033] Wenn das Terminal den Wert C_2, **28**, errechnet hat, erzeugt es eine geheime Zufallszahl R2, **29**, und sendet sowohl R2 als auch C_2, **32**, zur Karte. Die Karte führt dann die modulare Potenzierung **34** auf dem unterzeichneten Wert C_2 mit dem kleinen Exponenten T_e aus, wobei sie den Modul T_n des Terminals verwendet. Dies wird ausgeführt durch Errechnen von $R1' = C_2^{Te}$mod T_n. Wenn R1' gleich R1, **36**, ist, dann weiß die Karte, daß sie es mit einem Terminal zu tun hat, dessen ID T_{ID} mit dem Modul T_n assoziiert **38** ist. Generell enthält die Karte einen modulo-arithmetischen Prozessor (nicht gezeigt) zur Durchführung der obigen Operationen.

[0034] Die geheime Zufallszahl R2 wird von der Karte unterschrieben **40** und zum Terminal zurückgeschickt, zusammen mit einem von der CA unterzeichneten Zertifikat, das die ID der Karte zu der öffentlichen Information in Bezug setzt. Die Unterzeichnung durch die Karte erfolgt gemäß einem Unterschriftsalgorithmus mit elliptischer Kurve.

[0035] Die Verifizierung der Karte erfolgt auf ähnlicher Basis wie die Verifizierung des Terminals, jedoch erfolgt die Unterzeichnung durch die Karte unter Verwendung eines Verschlüsselungssystems mit elliptischer Kurve.

[0036] Typischerweise hat bei einer Umsetzung mit elliptischer Kurve eine Unterschriftskomponente s die Form:

$$2 = ae + k \pmod n$$

wobei gilt:

- P ist ein Punkt auf der Kurve, der ein vordefinierter Parameter des Systems ist;
- k ist eine zufällige ganze Zahl, die als kurzfristiger privater Schlüssel oder Sitzungsschlüssel gewählt wurde und einen entsprechenden kurzfristigen öffentlichen Schlüssel R = kP hat;
- a ist ein langfristiger privater Schlüssel des Senders (Karte) und hat einen entsprechenden öffentlichen Schlüssel aP = Q;
- e ist eine sichere Mischsumme, wie z. B. die SHA-Hash-Funktion, der Nachricht m (in diesem Falle R2) und des kurzfristigen öffentlichen Schlüssels R; und
- n ist die Ordnung der Kurve.

[0037] Zum Zwecke der Einfachheit wird angenommen, daß der Unterschriftsbestandteil die Form s = ae + k, wie oben diskutiert, hat, es ist jedoch ersichtlich, daß auch andere Unterschriftsprotokolle verwendet werden können.

[0038] Zur Verifizierung der Unterschrift muß sP – eQ errechnet und mit R verglichen werden. Die Karte generiert R z. B. unter Verwendung eines Feldarithmetik-Prozessors (nicht dargestellt). Die Karte sendet ein Nachricht an den Terminal, die m, s und R enthält, wie in Block **44** von **Fig. 2** gezeigt, und die Signatur wird durch das Terminal durch Errechnen des Wertes (sP – eQ), **46**, verifiziert, dieser Wert sollte kP entsprechen. Wenn die errechneten Werte einander entsprechen **48**, ist die Unterschrift verifiziert und damit auch die Karte, und die Transaktion kann fortgeführt werden.

[0039] Das Terminal überprüft das Zertifikat, dann die Unterschrift der Transaktionsdaten, die R2 enthält, und authentisiert damit die Karte für das Terminal. In der vorliegenden Ausführungsform ist die von der Karte generierte Unterschrift eine Unterschrift mit elliptischer Kurve, welche für die Karte einfacher zu generieren ist, jedoch einen größeren Rechenaufwand für die Verifizierung durch das Terminal erfordert.

[0040] Wie aus der obigen Gleichung ersichtlich ist, ist die Errechnung von s relativ einfach und erfordert keine bedeutende Rechnerleistung. Jedoch ist es zur Durchführung der Verifizierung notwendig, eine Anzahl von Punktmultiplikationen zu berechnen, um sP und eQ zu erhalten, die beide komplexe Berechnungen erfordern. Andere Protokolle, wie das MQV-Protokoll erfordern ähnliche Berechnungen, wenn sie über elliptischen Kurven umgesetzt werden, was bei begrenzter Rechenleistung zu langsamer Verifizierung führen kann. Dies ist jedoch bei Terminals im allgemeinen nicht der Fall.

[0041] Zwar wurde eine Ausführungsform unter Bezug auf ein spezifisches Protokoll für die Verifizierung des Terminals und für die Verifizierung der Karte beschrieben, andere Protokolle können jedoch auch verwendet werden.

Patentansprüche

1. Verfahren zur Verifizierung der Echtheit von zwischen einem Teilnehmerpaar in elektronischen Transaktionen über ein Datenübertragungssystem ausgetauschten Nachrichten, wo bei jeder der Teilnehmer Unterzeichnungs- und Verifizierungsteile eines ersten Unterschriftsschemas und eines zweiten Unterschriftsschemas, das sich vom ersten Unterschriftsschema unterscheidet und ein Verschlüsselungssystem mit elliptischer Kurve verwendet, aufweist, und wobei das Verfahren die folgenden Schritte umfasst:
die Unterzeichnung einer Nachricht durch einen der Teilnehmer gemäss einem Unterzeichnungsteil eines der Unterschriftsschemas, das mit dem Teilnehmer verbunden ist, um eine erste unterzeichnete Nachricht bereitzustellen, und Übertragung der ersten unterzeichneten Nachricht an den anderen der Teilnehmer; wobei der genannte andere Teilnehmer den Verifizierungsteil des genannten einen Unterschriftsschemas verwendet, um die von dem genannten einen Teilnehmer empfangene erste un terzeichnete Nachricht zu verifizieren;
die Unterzeichnung einer Nachricht durch den genannten anderen Teilnehmer unter Verwendung des genannten Unterzeichnungsteils des genannten anderen der Unterschriftsschemas, um eine zweite unterzeichnete Nach richt bereitzustellen, und Übertragung der zweiten unterzeichneten Nachricht an den genannten einen Teilnehmer;
die Verifizierung der von dem genannten anderen Teilnehmer empfangenen zweiten unterzeichneten Nachricht durch den genannten einen Teilnehmer unter Verwendung des Verifizierungsteils des genannten anderen der Unterschriftsschemas, wobei eine der Unterzeichnungen und eine der Verfizierungen gemäss dem zweiten Unterschriftsschema durchgeführt wird, das ein Verschlüsselungssystem mit elliptischer Kurve verwendet; und Verweigerung der Transaktion, falls eine der Verifizierungen misslingt.

2. Verfahren nach Anspruch 1, wobei beim ersten Unterschriftsschema die Unterzeichnung rechnerisch schwieriger ist als die Verifizierung, während beim zweiten Unterschriftsschema die Verifizierung rechnerisch schwieriger ist als die Unterzeichnung, wodurch es ermöglicht ist, dass einer der Teilnehmer mit relativ geringer Rechenleistung teilnehmen kann, während die Sicherheit der Transaktion bestehen bleibt.

3. Verfahren nach Anspruch 1, wobei das erste Digitalunterschriftsschema ein Schema vom RSA-Typ ist.

4. Verfahren nach Anspruch 1, wobei das erste Digitalunterschriftsschema ein Schema vom DSS-Typ ist.

5. Verfahren zur Verifizierung der Echtheit von zwischen einem Teilnehmerpaar in elektronischen Transaktionen über ein Datenübertragungssystem ausgetauschten Nachrichten, wobei jeder der Teilnehmer Unterzeichnungs- und Verifizierungsteile eines ersten Unterschriftsschemas und eines zweiten Unterschriftsschemas, das sich vom ersten Unterschriftsschema unterscheidet und ein Verschlüsselungssystem mit elliptischer Kurve verwendet, aufweist, und wobei das Verfahren das Verfahren nach Anspruch 1 anwendet und die folgenden Schritte umfasst:
Übertragung eines ersten Zertifikats durch den einen der Teilnehmer an den anderen der Teilnehmer, wobei das erste Zertifikat einen öffentlichen Schlüssel und Identifikationsinformation des genannten einen Teilnehmers enthält;
durch den genannten anderen Teilnehmer Verifizierung des Zertifikats und Extrahieren des öffentlichen Schlüssels und der Identifikationsinformation aus dem Zertifikat;
durch den genannten anderen Teilnehmer Erzeugen einer ersten Abfrage R_1 und Übertragung der Abfrage an den genannten einen Teilnehmer;
Unterzeichnen der empfangenen Abfrage R_1 gemäss dem Unterzeichnungsteil des einen der Unterschriftsschemas durch den genannten einen Teilnehmer, um eine zweite Unterschrift C_2 bereitzustellen;
durch den genannten einen Teilnehmer Erzeugen einer zweiten Abfrage und Übertragung der zweiten Abfrage zusammen mit der Unterschrift C_2 an den genannten anderen Teilnehmer;
Verifizierung der Unterschrift C_2 gemäss dem Verifizierungsteil des einen der Unterschriftsschemas durch den genannten anderen Teilnehmer;
durch den genannten anderen Teilnehmer Unterzeichnen der zweiten Abfrage R_2 gemäss dem Unterzeichnungsteil des anderen der Unterschriftsschemas, um ein weiteres Zertifikat bereitzustellen, und Übertragen des weiteren Zertifikats an den genannten einen Teilnehmer; und
Verifizierung des weiteren Zertifikats gemäss dem Verifizierungsteil des genannten anderen der Unterschriftsschemas durch den genannten einen Teilnehmer, und Verweigerung der Transaktion, falls die genannte Unterschrift nicht verifiziert wird.

6. Chipkarte zur Verwendung in einer elektronischen Transaktion mit einem Teilnehmer, wobei die Karte umfasst:
einen Speicher, enthaltend
einen Verifizierungsalgorithmus eines ersten Unterschriftsschemas, um eine Verifizierung einer durch den Teilnehmer gemäss einem ersten Unterschrifts-

generierungsalgorithmus ausgeführten Unterschrift durchzuführen;
einen Unterzeichnungsalgorithmus eines zweiten Unterschriftsschemas, das sich vom ersten Unterschriftsschema unterscheidet und ein Verschlüsselungssystem mit elliptischer Kurve verwendet, wobei der Unterzeichnungsalgorithmus eine Unterschrift gemäss einem zweiten Unterschriftsgenerierungsalgorithmus ausführt;
ein Programm zum Aufrufen der Algorithmen; und Rechnereinrichtungen zum Ablaufenlassen des Verifizierungsalgorithmus zur Verifizierung einer ersten, vom Teilnehmer unterzeichneten Nachricht und zum Ablaufenlassen des zweiten Unterschriftsgenerierungsalgorithmus zum Unterzeichnen einer zweiten Nachricht für die Übertragung an den Teilnehmer.

7. Chipkarte nach Anspruch 6, bei der der Verifizierungsalgorithmus eine RSA-Unterschrift verifiziert.

8. Chipkarte nach Anspruch 6, bei der der Verifizierungsalgorithmus eine DSS-Unterschrift verifiziert.

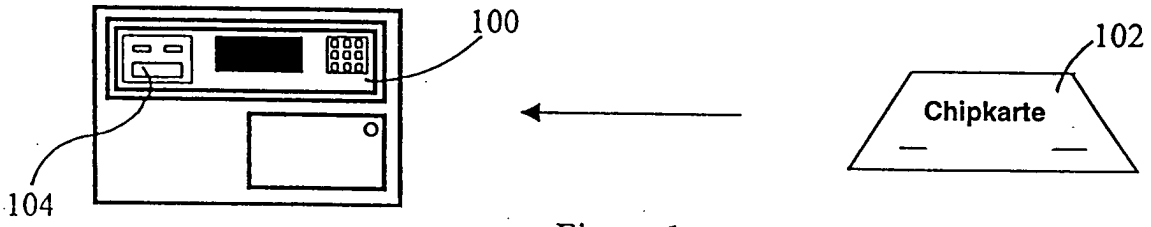
9. Nachricht, die als Datenstrom in einer elektronischen Transaktion über ein Datenübertragungssystem von einem ersten Teilnehmer an einen zweiten Teilnehmer gesandt wird, wobei jeder der Teilnehmer Unterzeichnungs- und Verifizierungsteile eines ersten Unterschriftsschemas und eines zweiten Unterschriftsschemas, das sich vom ersten Unterschriftsschema unterscheidet und ein Verschlüsselungssystem mit elliptischer Kurve verwendet, aufweist, und wobei die Nachricht umfasst:
a) einen ersten Wert R_2, der von der ersten Teilnehmer-Karte gemäss dem zweiten Unterschriftsschema unterzeichnet ist;
b) einen zweiten Wert, der von einer Zertifizierungsstelle gemäss dem ersten Unterschriftsschema unterzeichnet ist;
wobei der zweite Teilnehmer die Unterschrift beim zweiten Wert und dadurch die Unterschrift beim ersten Wert verifizieren kann.

10. Nachricht nach Anspruch 9, wobei beim ersten Unterschriftsschema die Unterzeichnung rechnerisch schwieriger ist als die Verifizierung, während beim zweiten Unterschriftsschema die Verifizierung rechnerisch schwieriger ist als die Unterzeichnung, wodurch es ermöglicht ist, dass der erste Teilnehmer mit relativ geringer Rechenleistung teilnehmen kann, während die Sicherheit der Transaktion bestehen bleibt.

11. Nachricht nach Anspruch 9, wobei das erste Unterschriftsschema ein Schema vom RSA-Typ ist.

Es folgen 2 Blatt Zeichnungen

Anhängende Zeichnungen



Figur 1a

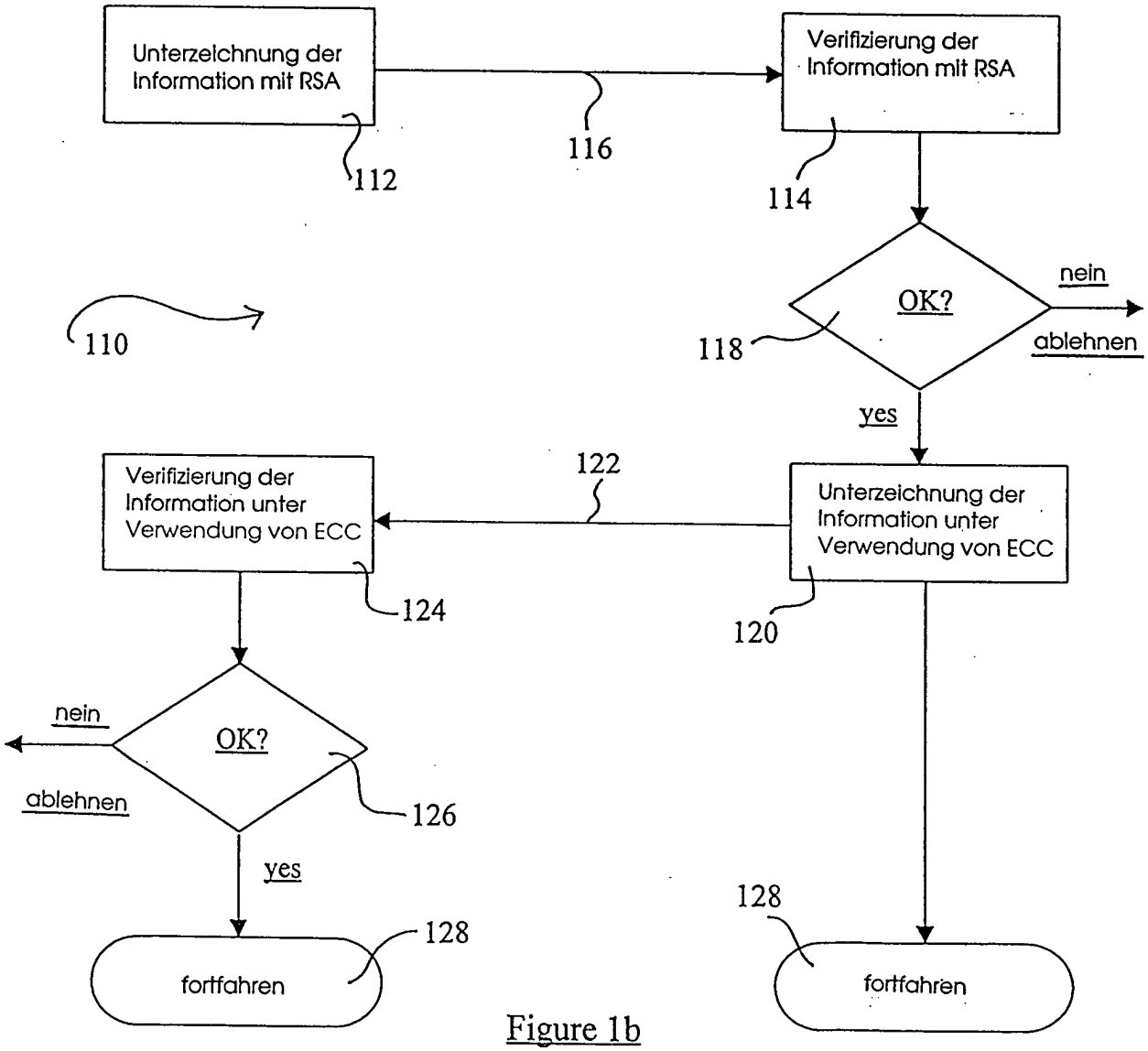
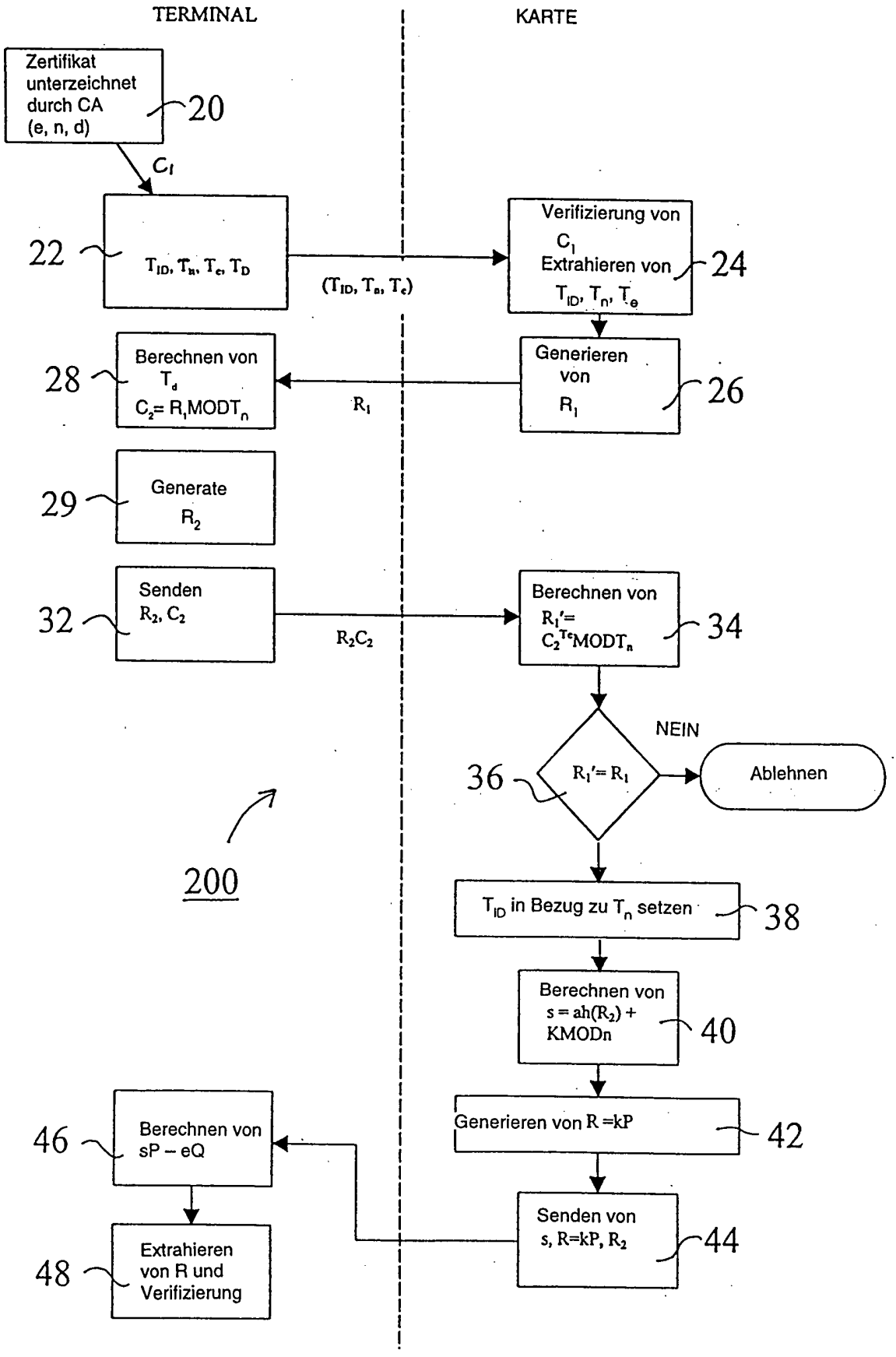


Figure 1b


TERMINAL
KARTE
Zertifikat unterzeichnet durch CA (e, n, d)
20
C_I
22
T_{ID}, T_n, T_e, T_D
(T_{ID}, T_n, T_e)
Verifizierung von C_I
Extrahieren von T_{ID}, T_n, T_e
24
Generieren von R_1
26
R_1
28
Berechnen von T_d
$C_2 = R_1 MOD T_n$
29
Generate R_2
32
Senden R_2, C_2
$R_2 C_2$
Berechnen von $R_1' = C_2^{T_e} MOD T_n$
34
NEIN
36
$R_1' = R_1$
Ablehnen
200
T_{ID} in Bezug zu T_n setzen
38
Berechnen von $s = ah(R_2) + KMODn$
40
Generieren von $R = kP$
42
Senden von $s, R=kP, R_2$
44
46
Berechnen von $sP - eQ$
48
Extrahieren von R und Verifizierung

FIGUR 2